PAT-NO: JP405303581A

DOCUMENT-IDENTIFIER: JP 05303581 A

TITLE: ELECTRONIC VOTING DEVICE

PUBN-DATE: November 16, 1993

INVENTOR-INFORMATION:
NAME
SAKO, KAZUE

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC CORP	N/A

APPL-NO: JP04108069

APPL-DATE: April 27, 1992

INT-CL (IPC): G06F015/28

ABSTRACT:

PURPOSE: To detect and exclude ineffective voting for both a positive and a negative vote by providing a means which totalizes votes unless a double vote is detected.

CONSTITUTION: A voter subsystem 101 reads the contents of a bulletin board 102 by using a bulletin board read means 301 and generates voting forms for a positive and a negative votes and double voting forms by using a constant number and a random number. A voting form converter 304 properly converts and sends them to a election administration center 100 through a signed vote transmitting means 305. The center 100 performs a blind sign processing and sends them back to voters 101. Each voter 101 generates voting contents and a

sign sentence for the double voting detection form by using the sent-back blind
sign sentence and sends the voting contents and double voting detection form to
the center 100 without the sign. The center 100 confirms voting contents in
adequate voting form with the adequate sign and the totalizing means 208
totalizes the voting contents unless double voting is detected.

COPYRIGHT: (C)1993,JPO&Japio

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－303581

(43)公開日　平成５年(1993)11月16日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ　15/28		Ｂ　7218－5Ｌ		

審査請求　未請求　請求項の数１(全　７　頁)

(21)出願番号　特願平4－108069

(22)出願日　平成４年(1992)４月27日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号日本電気株式会社内

(74)代理人　弁理士　京本　直樹　(外２名)

(54)【発明の名称】　電子投票装置

(57)【要約】

【目的】　電子的に無記名投票を行なうために、選挙管理センタによる集計洩れがあった場合も自分の投票内容を公表することなく集計洩れの異議申し立てを行なうことができる電子投票方式において、賛成にも反対にも投票する無効票検出方法の提案。

【構成】　投票を投票用設定フェーズと投票フェーズにより構成し、投票用紙設定フェーズにて投票内容に依存しない情報に対して選挙管理センタから署名をもらうときに、「二重投票検出用紙」についても署名をもらい、投票フェーズにおいては投票内容とこの「二重投票検出用紙」を提出する。

【効果】　二重投票検出用紙は一度しか有効にならないので、賛成・反対の双方に投票する無効票を検出でき、健全性の高い無記名電子投票装置が実現できる。

1

【特許請求の範囲】

【請求項1】　投票者が投票用紙と二重投票検出用紙とを変換して送出する投票用紙変換手段と、
選挙管理者が変換された投票用紙を検証する手段と、
選挙管理者が正当に変換された各投票用紙と二重投票検出用紙に対して署名をし、それを投票者に返信する署名手段と、
各投票者が返信された署名文を用いて投票内容と二重投票検出用紙に対する署名文を作成し、投票内容と二重投票検出用紙を署名付きで無記名で送付する投票手段と、正当な署名付きの正当な投票形式である投票内容であり、かつ二重投票が検出されなければ、その投票を集計する集計手段を有することを特徴とする電子投票装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は電子ネットワーク上で有権者だけが1度だけ無記名で投票でき、選挙管理センタの集計結果に対してプライバシーを尊重しつつ異議申し立てができる電子投票装置に関する。

【0002】

【従来の技術】電子投票方法として従来から知られているものは太田の方法がある。これは公開特許公報平1－177164及び昭和63年電子情報通信学会春季全国大会A－294「単一の選挙管理者を用いた電子投票方式」に開示されている。この方式は投票者は乱数で変換した投票内容に対してセンタの署名を得た後、乱数成分を取り除いた投票内容と投票内容に対する署名をセンタに送ることにより無記名投票を実現している。各投票者は自分の投票が集計されたことを、センタが発表する投票内容一覧で確認する。この方法では自分の意見を反映させた投票内容に対してのみセンタの署名を得られるので、センタがその投票内容を集計しなかった場合、自分の投票内容を公開して異議申し立てを行なわなくてはならない。

【0003】この問題を解決すべく、異議申し立てを行なう場合も、投票者が自分の投票内容を公開せずに異議申し立てを行なうために、あらかじめ投票用紙にのみ署名をもらい、署名付きの投票用紙に自分の意見を反映させた投票内容をセンタに送るという方式が考えられる。例えば、各有権者は賛成用・反対用両方の署名つき投票用紙を記名式で入手し、そのうち一方を無記名で投票する。

【0004】

【発明が解決しようとする課題】上述の方式において、賛成用・反対用の署名つき投票用紙を入手した有権者が選挙を崩壊させる目的で賛成・反対両方に投票する可能性がある。本発明ではこのような投票を無効にする電子投票装置を提案する。

【0005】

【課題を解決するための手段】本発明の電子投票装置

2

は、選挙管理者が変換された投票用紙を検証する手段と、選挙管理者が正当に変換された各投票用紙と二重投票検出用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票内容と二重投票検出用紙に対する署名文を作成し、投票内容と二重投票検出用紙を署名付きで無記名で送付する投票手段と、正当な署名付きの正当な投票形式である投票内容であり、かつ二重投票が検出されなければ、その投票を集計する集計手段を有することを特徴とする。

【0006】

【実施例】つぎに、図1から図4を参照して本発明の実施例について説明する。

【0007】本発明の電子投票装置を、図2のように、m個の投票者サブシステム101（1）～101（m）及び1つの選挙管理センタ100が相互に安全な通信チャネル（例えばデータ回線）105で結ばれており、さらに選挙管理センタ100のみが書き込み可能な掲示板で、すべての投票者サブシステムが読み出せる電子掲示板102が存在する場合の無記名電子投票システムに実施する例を述べる。なお、以下簡単のために選挙管理センタをセンタ、投票者サブシステムを投票者と呼ぶことにする。

【0008】また、本実施例では簡単のために投票内容は賛成あるいは反対の2値とするが、多値にも容易に拡張できる。

【0009】この投票システムは準備フェーズと、投票用紙設定フェーズ、投票フェーズおよび結果公表フェーズからなる。本発明は投票用紙設定フェーズ、第二次投票フェーズに関する。

【0010】まず、図3を持ちいて準備フェーズを説明する。

【0011】本無記名電子投票システムを実施するための準備として、センタ100は署名用の定数を設定し、検証用定数を電子掲示板102に掲示する。例えば、署名方式としてRSA暗号方式を用いるとする。そこで、素数p_iとq_iに対して$n_i = p_i \cdot q_i$（i＝1，0，2）とし、e_i，d_iを$e_i \cdot d_i = 1 \bmod (p_i - 1)(q_i - 1)$（i＝1，0，2）を満たす整数とする。このときセンタはe_i，n_i（i＝1，0，2）を検証用定数として設定する（ステップ11）。これらの定数を電子掲示板102に書き込む（ステップ12）。今後この検証用定数e_i，n_i（i＝1，0，2）は頻繁に用いられるので自分の定数保持手段201に書き込み容易にアクセスできるようにする（ステップ13）。一方、d_1，d_0，d_2は自分の秘密情報保持手段202に格納する（ステップ14）。

【0012】次に、センタ100は投票に関する規則を定める。まず、投票対象の議題を明らかにし、1組の賛成票・反対票・二重投票検出用紙のフォーマットを定める。たとえば、以下のような投票フォーマットを考え

る。ステップ11で設定されたn_j（j＝1，0，2）がそれぞれ512ビットであるとする。上位第1ビットから第8ビットに賛成票であるか、反対票であるかあるいは二重投票検出用紙であるかの種別を反映させ、全ビットの排他的論理和が1のとき賛成、0のとき反対とする。次に第9ビットから、第249ビットには乱数を発生させ、次の192ビットは、第1ビットから第56ビットをDES暗号の鍵、第57ビットから第249ビットを平文とみなした場合の暗号文とするフォーマットとする（ステップ15）。　次に、投票する権利のあるサブシステム（以後、有権者と呼ぶ）の名前を一覧にする（ステップ16）。投票用紙作成及び投票の期限を設定・公表し（ステップ17）、投票用紙作成フェーズの開始を合図する（ステップ18）。

【0013】以上が準備フェーズである。

【0014】次に、投票用紙作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ100は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム101（i）に対する手順を例にとって説明を続ける。

【0015】図1に示すように無記名電子投票システムはセンタ100が電子掲示板102に定数及び投票規則を書き込む安全通信チャネル103、投票者101（i）が電子掲示板102に書かれた内容を読み出すための安全通信チャネル104（i）および投票者とセンタが交信するための安全通信チャネル105（i）で構成されている。

【0016】まず、図1を参照しながら投票者101（i）の第一次投票フェーズを説明する。

【0017】投票者101（i）は提示板読み出し手段301を用いて掲示板102に書かれてある内容を読み出し、定数e_j，n_j（j＝1，0，2）を定数保持手段302に格納する一方、読み出したフォーマットに沿うよう投票用紙作成手段310にて賛成票・反対票の投票用紙V_1（i），V_0（i）と二重投票検出用紙V_2（i）を生成する。なお、各賛成票・反対票及び二重投票検出用紙作成にあたって投票フォーマットに必要な乱数成分は乱数発生器303の出力を用いる。

【0018】次に、投票用紙変換器は、乱数発生器303の出力r_bと定数e_b，n_b（b＝1，0，2）を用いて、

【0019】

【数1】

$$S_b(i)=V_b(i)\cdot r_b^{e_b} \bmod n_b$$

$$S_b=V_b\cdot r_b \bmod n_b$$

【0020】を計算し、s_1（i），s_0（i），s_2（i）を出力する。また、このときの乱数発生器303の出力r_bは乱数保持器309に格納する。s_1（i），s_0（i），s_2（i）を記名付き送信手段305が安全チャネル105（i）を通じてセンタ100に送信する。

【0021】センタ100は投票用紙受信手段206で、受信した該投票用紙s_1（i），s_0（i）およびs_2（i）を公表手段303で掲示板に公開すると共に、署名生成器204で署名を以下のように行なう。

【0022】ブラインド署名生成器204は秘密保持手段201、定数保持手段202から読みだしたd_b及びn_bを用いて、

D_b（i）＝s_b（i）$^{d_b} \bmod n_b$

を各b＝1，0，2について計算し、出力する。ブラインド署名送信手段205はD_b（i）を投票者101（i）に送信する。

【0023】投票用紙作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上が投票用紙設定フェーズである。

【0024】次に、投票フェーズを説明する。

【0025】署名検証手段306は、ブラインド署名受信手段311によりセンタ100から受信したD_b（i）と、定数保持手段302から読み出したe_b，n_bを用いて

S_b（i）＝D_b（i）$^{e_b} \bmod n_b$

が各b＝1，0，2について成立するかどうか検証する。また、自分の第一次投票内容s_b（i）が掲示板に記載され、数えられていることを確認する。

【0026】確認できれば、投票生成器307は、自分の意見B（Bは0か1）に対して、乱数保持器309から読み出した整数r_B，r_2と、定数保持手段302から読み出したn_B，n_2を用いて、

t_B（i）＝D_B（i）／$r_B \bmod n_B$

t_2（i）＝D_2（i）／$r_2 \bmod n_2$

を計算し、無記名送信手段308はB，t_B（i），t_2（i）を送信者名を付記せずにセンタ100に送出する。

【0027】センタ100は、投票確認手段で、

【0028】

【数2】

$$t_B(i)^{e_B} \bmod n_B$$

$$t_2(i)^{e_2} \bmod n_2$$

【0029】を計算し、その出力、すなわち投票内容及び二重投票検出用紙があらかじめ掲示板に記載されたフォーマットに従っているか否かを検証する。なお、この値は投票者が不正をしていなければ、それぞれv_B（i），v_2（i）に等しくなる。

【0030】さらに、投票内容及び二重投票検出用紙が共に以前に投票されていないことを確認する。投票されていれば無効票とみなす。そのようなことがなければその投票内容を集計手段208で集計する。

5

【００３１】以上が投票フェーズである。

【００３２】投票フェーズのバリエーションとして、無記名送信手段がＢを送らずともtB（ｉ），t2（ｉ）のみを送ることもできる。このとき、センタ１００は投票検証手段２０７で、

$t_B(i)^{e_B} \bmod n_B$

の結果がＢ＝１，０どちらの時に正当な投票に内容になるかを検証すれば良い。

【００３３】全員の投票が終了すれば結果公表フェーズとして、センタは無記名で送付されたすべての投票を掲示板に列挙し、集計結果を公表する。各有権者は自分の投票が正しく記載されていることと、記載されている投票を集計すると確かに公表された集計結果になることを確認する。

6

＊【００３４】ここでもし自分の投票が記載されていないとすると、センタから受信した$D_b(i)$（ｂ＝１，０，２）を用いて

$t_b(i)=D_b(i)/r_b \bmod n_b$

をｂ＝１，０，２に関して公表し、b_1，b_2 あるいは b_0，b_2 のどちらも計上されていないことを示すことによって異議申し立てを行なう。自分の投票を公開するのではなく投票用紙を公開するのでプライバシーを保った異議申し立てが行なえる。

【００３５】さらに$n_1=n_0=n_2$，$e_1=e_0=e_2$，$d_1=d_0=d_2$ とすることもできる

【００３６】

【数３】

＊

また、本発明を選択肢が賛成・反対の二種しかない投票ではなく、一般に多値の場合も以下のようにして効率良く行なうことができる。

選択肢が2^k個あったとする。このとき、センタは２ｋ＋１個のＲＳＡ用の定数$n_1^{(1)}$，$n_1^{(2)}$，…，$n_1^{(k)}$，$n_0^{(1)}$，$n_0^{(2)}$，…，$n_0^{(k)}$，$n_\beta^{(0)}$を２つの素数の積として設定し、公開鍵$e_1^{(1)}$，$e_1^{(2)}$，…，$e_1^{(k)}$，$e_0^{(1)}$，$e_0^{(2)}$，…，$e_0^{(k)}$，$e_\beta^{(0)}$および秘密鍵$d_1^{(1)}$，$d_1^{(2)}$，…，$d_1^{(k)}$，$d_0^{(1)}$，$d_0^{(2)}$，…，$d_0^{(k)}$，$d_\beta^{(0)}$をそれぞれ（$n_b^{(1)}$，$e_b^{(1)}$，$d_b^{(1)}$）がＲＳＡ署名系を構成するよう設定する。

投票は選択肢の番号の各ビットを選択することにより投票する。すなわち、１ビット目が１の時$v_1^{(1)}$、０の時$v_0^{(1)}$を提出するとする。そこで投票用紙を$v_1^{(1)}$，$v_1^{(2)}$，…，$v_1^{(k)}$，$v_0^{(1)}$，$v_0^{(2)}$，…，$v_0^{(k)}$とし、$v_\beta^{(0)}$を二重投票検出用紙とする。投票用紙設定フェーズではこれらを各々変換してセンタに署名してもらい、変換前の署名を得る。

次に投票フェーズにおいては、選択肢の番号$C=\sum_1^k c_i \cdot 2^{i-1}$に対して、

$$v_{c_i}^{(i)} \quad (i=1,\cdots k)$$

および$v_\beta^{(0)}$を署名つきで送ればよい。

上記のようにすれば、選択肢の数の対数に比例した通信量で本発明を実現できる。同様に、選択肢の数がq^kのとき、通信量はｑ・ｋに比例することがわかる。

なお、ここで$n_i^{(j)}$，$e_i^{(j)}$，$d_i^{(j)}$を一部共通に使うこともできる。

【００３７】図４を参照すると、このシステムは、通信処理機能を備えたパーソナルコンピュータ等の端末装置（ＴＭＵ）４０１と、読出し専用記憶装置（ＲＯＭ）４０２と、ランダムアクセス記憶装置（ＲＡＭ）４０３と、乱数発生器（ＲＮＧ）４０４と、シグナルプロセッ※サ（ＳＰ）４０６と、ＴＭＵ４０１、ＲＯＭ４０２、ＲＡＭ４０３、ＲＮＧ４０４およびＳＰ４０６を相互に接続する共通バス４０５とから構成される。

【００３８】ＲＮＧ４０４は乱数をＳＰ４０６の指令により発生する。これはセンタ１００が定数設定の時に用

い、また各投票者１０１（ｉ）の乱数発生器として用いる。ＲＯＭ４０７にはセンタ１００の場合、定数e_1，n_1，e_0，n_0，e_2，n_2，と秘密情報d_1，d_0，d_2を記憶している。d_1，d_0，d_2はＴＭＵからブラインド署名作成の度にＲＡＭに格納するようにしてもよい。ＲＯＭ４０７には投票者サブシステム１０１（ｉ）の場合、定数e_j，n_j（ｊ＝１，０，２）を記憶している。ＲＯＭ内に格納されたプログセラムに基づいて、上述の動作を実現する。ＲＡＭ４０３はこれらのステップの実行中に計算途中結果等を一時的に記憶するために用いられる。

【００３９】また、システム１００，１０１（ｉ）は汎用電子計算機のデータ処理装置やＩＣカードであってもよい。

【００４０】

【発明の効果】以上詳細に説明したように、本発明を用いれば、プライバシーを保ったまま異議申し立てができる無記名電子投票システムにおいて、賛成・反対の両方に投票する無効表を検出することができる。

【図面の簡単な説明】

【図１】本発明の電子投票装置の位置実施例を示すブロック図。

【図２】無記名電子投票システムを示す図。

【図３】準備フェーズの例を示す図。

【図４】センタ１００、投票者サブシステム１０１（ｉ）の構成を示す図。

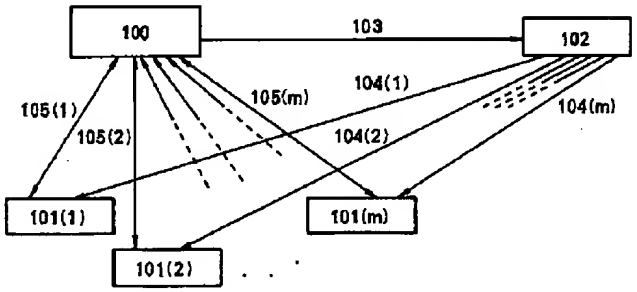
【符号の説明】

１００　選挙管理センタ

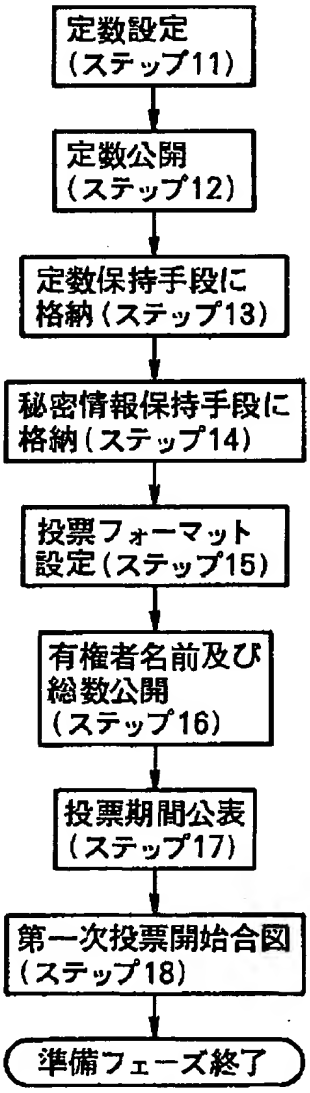
１０１（ｉ）　投票者サブシステム

１０２　電子掲示板

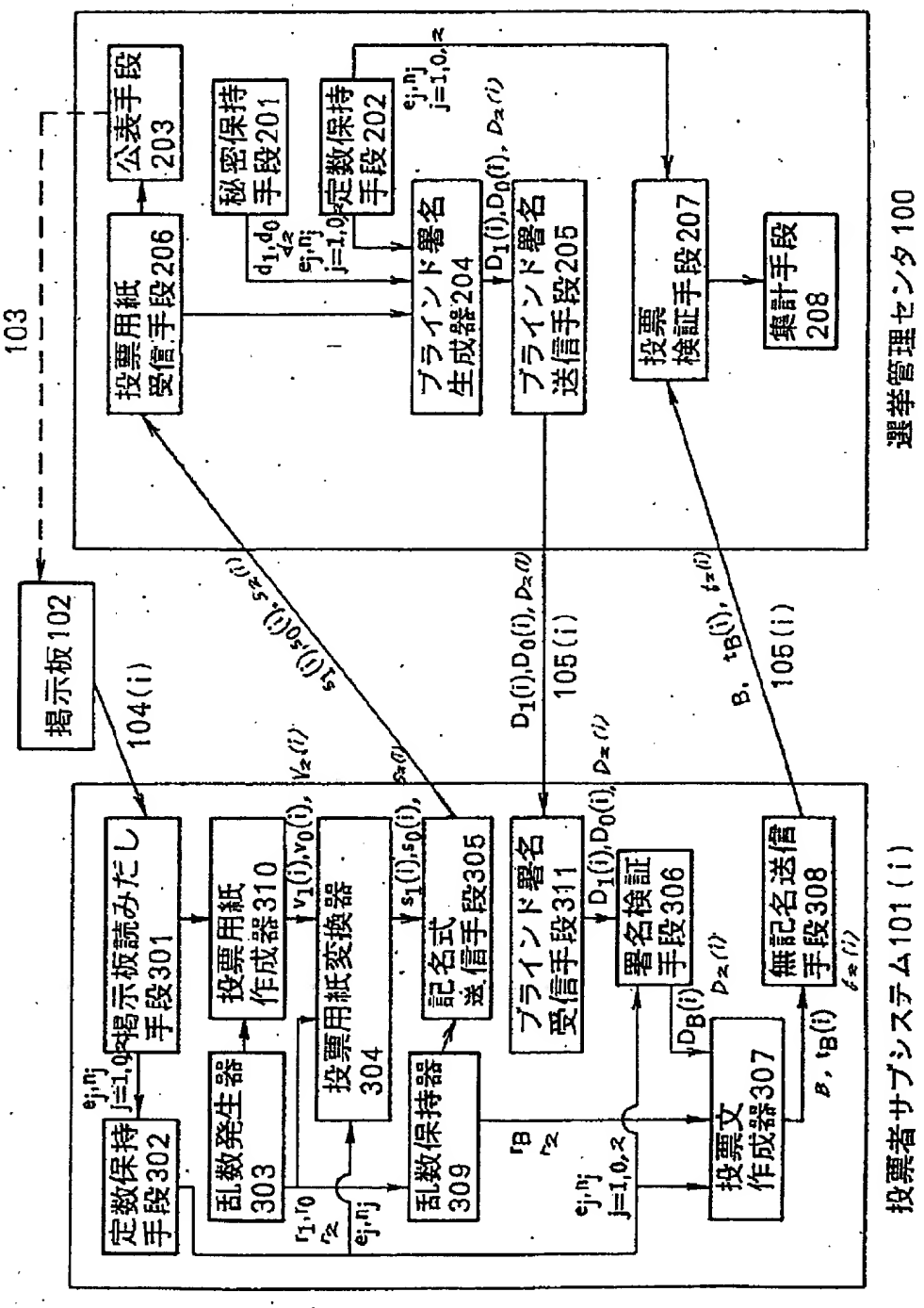
【図２】



【図３】



【図1】


選挙管理センタ100
公表手段203
秘密保持手段201
定数保持手段202
投票用紙受信手段206
ブラインド署名生成器204
ブラインド署名送信手段205
投票検証手段207
集計手段208
103
掲示板102
104(i)
105(i)
投票者サブシステム101(i)
掲示板読みだし手段301
定数保持手段302
乱数発生器303
投票用紙作成器310
投票用紙変換器304
乱数保持器309
記名式送信手段305
ブラインド署名受信手段311
署名検証手段306
投票文作成器307
無記名送信手段308

【図4】